Notice of Allowability	Application No.	Applicant(s)	
	09/854,666	UCHIDA, KAORU	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *1 December 2006 and 27 February 2007*.

2. ☒ The allowed claim(s) is/are *1,3-11,13-20,22,23,25,26 and 28-31*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☒ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☒ Certified copies of the priority documents have been received in Application No. *09/854,666* .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 13 October 2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *2/27/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

1. In response to amendment after filed on 1 December 2006 and Examiner Initiated Interview on 27 February 2007.

Information Disclosure Statement

2. The information disclosure statement filed 13 October 2006 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because no English translation provided about the foreign patents or other documents not in English, or portion identified and translated about the portion of Patents that is relevant. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Reasons for Allowance

3. Claims 1, 3-11, 13-20, 22, 23, 25, 26, and 28-31 are allowed over the prior art of record.

The following is a statement of reasons for the indication of allowable subject matter:

In interpreting the claims in light of the specification and applicant's arguments. Examiner finds the claimed invention is patentable distinct from the prior art of record.

The prior art of record, Musgrave discloses a technique for combining biometric identification with digital certificates for electronic authentication called biometric certificates. Biometric certificates may be used in an any electronic transaction requiring authentication of the participants. The prior art of record Matyas discloses methods, systems, and computer

program products which allow for multi-party authentication by receiving a plurality of biometric authentication messages from a corresponding plurality of users. The prior art of record Glass discloses a method and apparatus for collecting and securely transmitting biometric data over a network associated with a unique code that identifies the sensor or time, or a time interval data is considered valid, or a unique transaction code.

The prior art of record, Musgrave in view of Matyas in further view of Glass fail to anticipate or render Applicant's particular feature that

> **"wherein each one of the plurality of ECSP units receives a transaction request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via a communications network and for each received transaction request message, one of the plurality of ECSP units transmits an authentication request message containing said ciphered biometrics data and said user identifier to said network; and an authentication server comprising a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifier, wherein the authentication server receives the authentication request messages from the plurality of ECSP units via said network and for each of the received authentication request messages, the authentication server decipheres the ciphered biometrics data"**
> As stated in claim 1, or similarly stated in claims 11, 20, 22, 26, 28, 29, 30, and 31

The dependent claims, being further limiting to the independent claims, defined and enabled by the Specification are also allowed.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
23 February 2007

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

1. (previously presented): An identification system comprising:

a plurality of end terminals,

a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a transaction request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via a communications network and for each received transaction request message, one of the plurality of ECSP units transmits an authentication request message containing said ciphered biometrics data and said user identifier to said network; and

an authentication server comprising a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, wherein the authentication server receives the authentication request messages from the plurality ECSP units via said network, and for each of the received authentication request messages, the authentication server decipheres the ciphered biometrics data and compares the deciphered biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in the received authentication request message and returns a reply to the plurality of ECSP units via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

2. (canceled).

3. (previously presented): The identification system of claim 1, wherein each one of the plurality of ECSP units includes a conversion table for mapping a first plurality of user identifiers to a second plurality of user identifiers, wherein said first plurality of user identifiers are used by said plurality of end terminals and said second plurality of user identifiers are the user identifiers registered in said database, each one of the plurality of ECSP units converts the user identifier contained in the received transaction request message to one of the second plurality of user identifiers which is mapped to the received user identifier and transmits said authentication request message containing the converted user identifier.

4. (previously presented): The identification system of claim 1, wherein each of said end terminals is configured to generate said ciphered biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server.

5. (previously presented): The identification system of claim 4, wherein said variable secret key generator is located at said authentication server and wherein each of said end terminals is configured to transmit a key request message to said authentication server via said plurality of ECSP units, to receive said secret key from the secret key generator: and to ciphering a biometrics data with the received secret key before said transaction request message is transmitted.

6. (original): The identification system of claim 5, wherein said authentication server comprises a variable secret key generator which generates a secret key which varies with time, and a decryption unit for deciphering the received ciphered biometrics data by using the secret key generated by said secret key generator.

7. (original): The identification system of claim 1, wherein each of said end terminals comprises a user terminal exclusively owned by said user.

8. (previously presented): The identification system of claim 1, wherein each of said end terminals comprises a sales terminal to which a plurality of user's handheld personal units can be connected, wherein said sales terminal transparently transmits a transaction request messaged received from each of the personal units to said plurality of ECSP units.

9. (original): The identification system of claim 1, wherein said biometrics data of said user is a fingerprint of said user.

10. (original): The identification system of claim 1, wherein said biometrics data of said user is an extracted feature of a fingerprint of said user.

11. (previously presented): An identification system comprising:

a plurality of end terminals

a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a transaction request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via a communications network and for each received transaction request message, one of the plurality of ECSP units transmits an authentication request message containing said ciphered biometrics data to said network: and

an authentication server comprising a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, wherein the authentication server receives the authentication request messages from the plurality of ECSP units via said network, comparing and for each of the received authentication request messages,

the authentication server deciphers the ciphered biometrics data and compares the deciphered biometrics data to all of the registered biometrics data in said database, detects the user identifier mapped to the registered biometrics data which coincides with the deciphered biometrics data, and returns a reply to the plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated.

12. (canceled).

13. (previously presented): The identification system of claim 11, wherein each of said end terminals is configured to generate said ciphered biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server.

14. (previously presented): The identification system of claim 13, wherein said variable secret key generator is located at said authentication server and wherein each of said end terminals is configured to transmit a key request message to said authentication server via said plurality of ECSP units to receive said secret key from the secret key generator: and to cipher a biometrics data with the received secret key before said transaction request message is transmitted.

15. (original): The identification system of claim 14, wherein said authentication server comprises a variable secret key generator which generates a secret key which varies with time, and a decryption unit for deciphering the received ciphered biometrics data by using the secret key generated by said variable secret key generator.

16. (previously presented): The identification system of claim 11, wherein each of said end terminals comprises a user terminal exclusively owned by said user.

17. (previously presented): The identification system of claim 11, wherein each of said end terminals comprises a sales terminal to which a plurality of user's handheld personal units can be connected, wherein said sales terminal transparently transmits a transaction request messaged received from each of the personal units to said plurality of ECSP units.

18. (original): The identification system of claim 11, wherein said biometrics data of said user is a fingerprint of said user.

19. (original): The identification system of claim 11, wherein said biometrics data of said user is an extracted feature of a fingerprint of said user.

20. (previously presented): An identification method comprising the steps of:

a) transmitting, from a plurality of end terminals, transaction request messages, containing ciphered biometrics data of a user to a communications network;

b) receiving, at each one of a plurality of electronic commerce service providers, one of the transaction request messages via said network;

c) for each received transaction request message, transmitting, an authentication request message containing said ciphered biometrics data from one of the plurality of electronic commerce service provider units to said network;

d) receiving said authentication request messages via said network at a user authenticator having a database for storing a plurality of registered biometrics data and the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, determining whether the deciphered biometrics data has corresponding biometrics data in said database; and

f) for each of the received authentication request messages, returning a reply from said user authenticator to said plurality of electronic commerce service provider via said network indicating that said transaction request message is authenticated if the received deciphered biometrics data coincides with one of the registered biometrics data of the database.

21. (canceled).

22. (previously presented): An identification method comprising the steps of:

a) transmitting, from a plurality of end terminals, transaction request messages, each transaction request message containing ciphered biometrics data of a user and a user identifier of said user to a communications network;

b) receiving, at each one of a plurality of electronic commerce service providers, one of said transaction request messages via said network;

c) for each of the received transaction request messages, transmitting, an authentication request message containing said ciphered biometrics data and said user identifier from one of the plurality of electronic commerce service provider units to said network;

d) receiving said authentication request messages at a user authenticator via said network, the authenticator having a database in which a plurality of registered biometrics data are mapped to a plurality of corresponding registered user identifiers and deciphering the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, comparing the deciphered biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in said authentication request message; and

f) for each of the received authentication request messages, returning, from the user authenticator, a reply to said plurality of electronic commerce service providers via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

23. (previously presented): The identification method of claim 22, wherein the user identifiers stored in said database are different from the user identifiers of said end terminals, further comprising converting, at each one of the plurality of electronic commerce service providers, the user identifier contained in the received transaction request message to a second user identifier which is contained in said authentication request message as the first-mentioned user identifier.

24. (canceled).

25. (previously presented): The identification method of claim 22, wherein a biometrics data contained in the transaction request message is ciphered by using a secret key which varies with time and agrees with the secret key with which the ciphered biometrics data is deciphered at said user authenticator.

26. (previously presented): An identification method comprising the steps of:

a) transmitting, from a plurality of end terminals, transaction request messages, each transaction request message containing ciphered biometrics data of a user to a communications network;

b) receiving, at each one of a plurality of electronic commerce service providers, one of said transaction request message via said network;

c) for each of the received transaction request messages, transmitting, an authentication request message containing said ciphered biometrics data from one of the plurality of electronic commerce service providers to said network;

d) receiving, at a user authenticator having a database in which a plurality of registered biometrics data are mapped to a plurality of corresponding registered user identifiers, said authentication request messages via said network and deciphering the ciphered biometrics data contained in the received authentication request messages;

e) for each of the received authentication request messages, comparing the deciphered biometrics data to all of the registered biometrics data in said database to detect coincidence;

f) for each of the received authentication request messages, detecting the user identifier mapped to the biometrics data which coincides with the deciphered biometrics data; and

g) for each of the received authentication request messages, returning a reply from the user authenticator to said plurality of electronic commerce service providers via said network indicating that said user having the detected user identifier is authenticated.

27. (canceled).

28. (previously presented): An identification system comprising:

a plurality of terminals,

a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a registration request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via a communications network, retransmits the registration request message to said network, receives a transaction request message containing said ciphered biometric data and

user identifier transmitted from the plurality of end terminals via said network, and for each received transaction request message, transmits an authentication request message containing said biometrics data and said user identifier to said network; and

an authentication server for receiving said registration request messages from said plurality of ECSP units via said network, mapping in a database a plurality of biometric data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contain in said registration request messages, the authentication server further receiving the authentication request messages from the plurality of ECSP units via said network, and for each of the received authentication request messages, the authentication server deciphers the ciphered biometrics data and compares, the received deciphered biometrics data to one of the biometrics data which is mapped in said database to the user identifier contained in the received authentication request message and returns a reply to said the plurality of ECSP units via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data.

29. (previously presented): An identification system comprising:

a plurality of end terminals,

a plurality of electronic commerce service provider (ECSP) units, wherein each one of the plurality of ECSP units receives a registration request message containing ciphered biometrics data of a user and a user identifier of said user transmitted from the plurality of end terminals via a communications network, retransmits the registration request message to said network, receives a transaction request message containing said ciphered biometrics data transmitted from the plurality of end terminals via said network, and for each received

transaction request message, transmits an authentication request message containing said ciphered biometrics data and said user identifier to said network; and

an authentication server for receiving said registration request messages from said plurality of ECSP units via said network, mapping a plurality of biometrics data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contained in said registration request messages, the authentication server receiving the authentication request messages from the plurality of ECSP units via said network, and for each of the received authentication request messages, the authentication server decipheres the ciphered biometrics data and compares comparing the received and deciphered biometrics data to all of the biometrics data in said database, detects the user identifier mapped to the biometrics data which coincides with the received biometrics data, and r4mmain~returns a reply to said plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated.

30. (currently amended): An authentication server comprising:

a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers;

an interface unit for receiving authentication request messages from a plurality of electronic commerce service provider (ECSP) units via a network, each authentication request message containing ciphered biometrics data of a user and a user identifier of said user; ~~and~~

a deciphering unit which deciphers the ciphered biometrics data; and

a processor, wherein for each of the received authentication request messages, the processor compares the ~~received~~ deciphered biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in the received authentication request message,

wherein the interface unit returns a reply to the plurality of ECSP units via said network indicating that the transaction request message is authenticated if the ~~received~~ deciphered biometrics data coincides with the said mapped biometrics data,

wherein each authentication request message corresponds to a transaction request message transmitted to one of the plurality of ECSP units from one of a plurality of user terminals via said network.

31. (currently amended): An authentication server comprising:

a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers;

an interface unit for receiving authentication request messages from a plurality of electronic commerce service provider (ECSP) units via a network, each authentication request message containing ciphered biometrics data of a user and a user identifier of said user; ~~and~~

a deciphering unit which deciphers the ciphered biometrics data; and

a processor, wherein for each of the received authentication request messages, the processor compares the ~~received~~ deciphered biometrics data to all of the registered biometrics data in said database and detects the user identifier mapped to the biometrics data which coincides with the ~~received~~ deciphered biometrics data,

wherein the interface unit returns a reply to the plurality of ECSP units via said network indicating that a user identified by the detected user identifier is authenticated,

wherein each authentication request message corresponds to a transaction request message transmitted to one of the plurality of ECSP units from one of a plurality of user terminals via said network.

KAMBIZ ZAND
PRIMARY EXAMINER